DATENBLATT:

proofpoint.

PROOFPOINT CLOUD ACCOUNT DEFENSE

Proofpoint Cloud Account Defense (PCAD) schützt Microsoft Office 365-Benutzer vor Kontenkompromittierung. Mit PCAD können Sie Cyberkriminelle, die es auf Ihre vertraulichen Daten und vertrauenswürdigen Konten abgesehen haben, entdecken, untersuchen und abwehren. Unsere umfangreiche Forensik sowie die richtlinienbasierten Kontrollen helfen Ihnen bei der Überwachung und Behebung anhand der Risikofaktoren, die für Sie relevant sind.

WICHTIGE VORTEILE

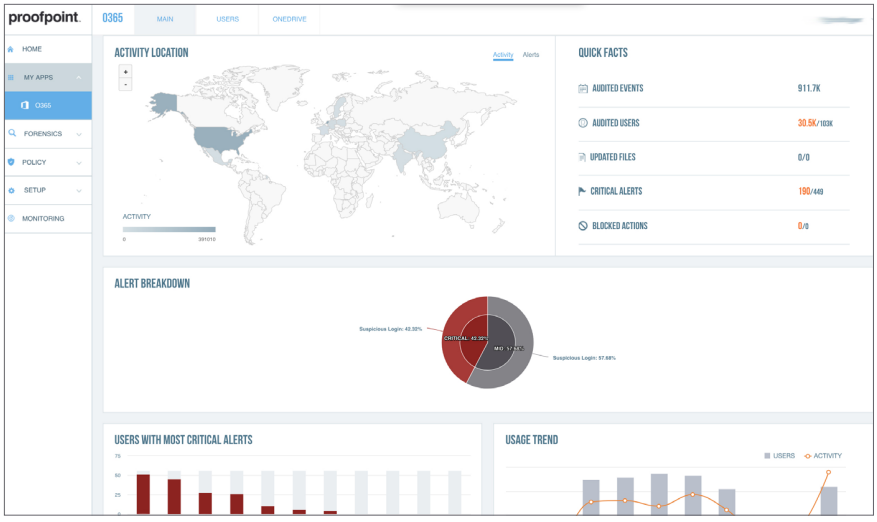
- Identifizierung der gefährdetsten Benutzer und Überwachung auf Zwischenfälle über aufschlüsselbare Dashboards
- Anpassung und Priorisierung von Warnungen basierend auf den für Sie relevanten Risikofaktoren
- Korrelation von E-Mail- und Cloud-Bedrohungen zur zuverlässigen Erkennung kompromittierter Konten
- Untersuchung von Sicherheitszwischenfällen durch umfangreiche Forensik und anpassbare Berichte
- Automatisierung der Sicherheitsreaktionen mithilfe flexibler Richtlinienkontrollen
- Schnelle Bereitstellung in der Cloud
- Zuverlässiger preisgekrönter Kunden-Support

Die Anmeldedaten Ihrer Benutzerkonten sind der Schlüssel zum Königreich Ihres Unternehmens. Wenn Cyberkriminelle diese Anmeldedaten Ihrer Office 365-Konten kompromittieren, können sie Angriffe von inner- und außerhalb Ihres Unternehmens starten und Benutzer davon überzeugen, Geld zu überweisen oder vertrauliche Informationen weiterzugeben. Zudem erhalten sie so möglicherweise Zugriff auf Ihre wichtigen Daten, z. B. Ihr geistiges Eigentum oder Kundendaten. Das schadet nicht nur dem Ruf, sondern auch den Finanzen Ihres Unternehmens. Und sobald die Angreifer einen Fuß in der Tür haben, installieren sie häufig Backdoor-Trojaner für zukünftige Angriffe. Die Kontenkompromittierung erfolgt zwar häufig per Phishing, aber auch mit folgenden Methoden:

- Brute-Force-Angriffe, bei denen die Anmeldedaten automatisiert „erraten“ werden
- Wiederverwendung von Anmeldedaten, wobei zuvor gestohlene Benutzernamen- und Kennwort-Paare verwendet werden
- Malware wie Keylogger-Programme und Anmeldedaten-Diebe

Mit unserem integrierten Ansatz, der die Menschen in den Mittelpunkt stellt und Cloud- sowie E-Mail-Aktivitäten korreliert, können Sie Ihre Office 365-Konten vor Kompromittierung schützen. Wir kombinieren Analysen des Cloud-Zugriffs sowie des Benutzerverhaltens mit unseren E-Mail-Bedrohungsdaten. Dadurch können Sie gefährdete Benutzer sowie kompromittierte Konten erkennen.

ERKENNUNG KOMPROMITTIERTER KONTEN

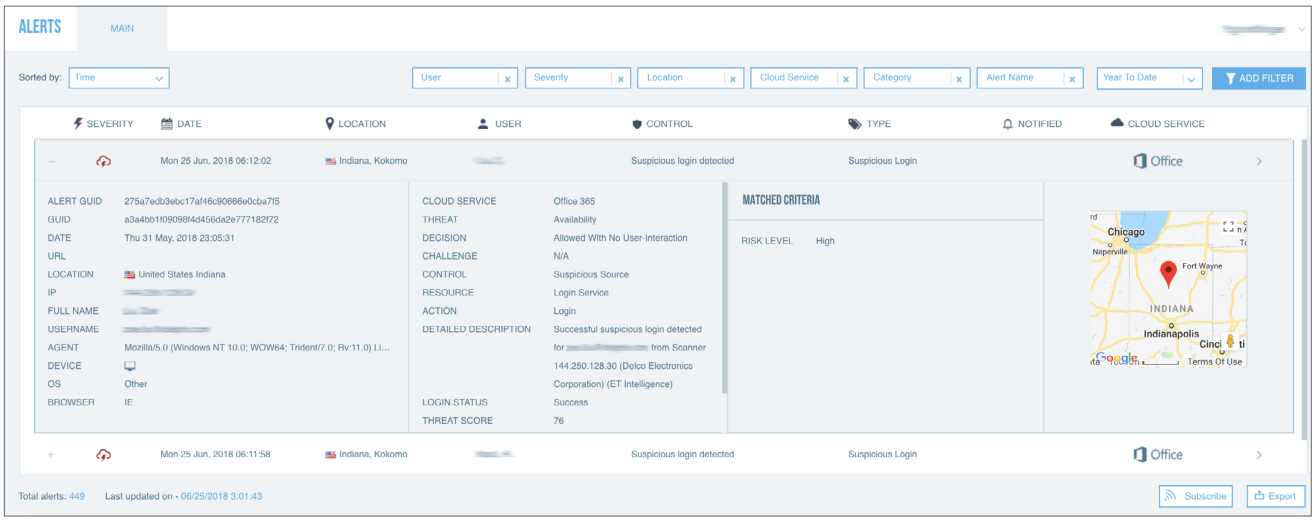


Für die Erkennung kompromittierter Konten nutzt PCAD Kontextdaten wie Benutzerstandort, Gerät, Netzwerk und Anmeldezeitpunkt. Wir etablieren mithilfe von Analysen Basislinien und suchen anhand von erfassten Spuren, Schwellenwerten und hochentwickeltem Machine Learning nach Anomalien. Wir suchen nach verdächtigen Aktivitäten wie extrem häufigen und ungewöhnlichen Anmeldeversuchen, zum Beispiel nach typischem Brute-Force-Verhalten und Ereignissen, die objektiv zu schnell aufeinander erfolgen.

Zudem kombiniert PCAD unsere umfangreichen Bedrohungsdaten mit benutzerspezifischen Risikoindikatoren. Dadurch können Sie Anmeldeversuche aus ungewöhnlichen Quellen erkennen. Wir setzen unsere globalen Bedrohungsdaten auch für Reputationsprüfungen von IP-Adressen ein und korrelieren Bedrohungsaktivitäten von E-Mails bis zur Cloud. Zudem helfen unsere E-Mail-basierten Bedrohungsdaten, E-Mail-Angriffe per Anmeldedaten-Phishing und verdächtige Anmeldeversuche in Beziehung zu setzen. Angreifer können ein kompromittiertes Konto für einen Phishing-Angriff nutzen und andere Benutzer in Ihrem Unternehmen kompromittieren. Um weitere kompromittierte Konten zu identifizieren, untersuchen wir die Spuren des Angreifers auf ungewöhnliche Benutzeragenten und Aktivitäten (z. B. E-Mail-Weiterleitungen).

UNTERSUCHUNG VON ZWISCHENFÄLLEN MIT DETAILLIERTER FORENSIK

Wenn es zu einem Zwischenfall kommt, können Sie in unserem intuitiven Dashboard frühere Aktivitäten und Warnungen untersuchen. Hier können Sie detaillierte Forensikdaten zu Transaktionen überprüfen, z. B. Benutzer, Datum und Uhrzeit, IP-Adresse, Gerät, Browser, Benutzeragent, Standort, Bedrohung und Bedrohungsbewertung sowie viele weitere. Ebenso lassen sich diese Daten in aufschlüsselbaren Grafiken und Protokollberichten anzeigen und analysieren. Außerdem können Sie Aktivitäts- und Warnungsprotokolle filtern und sortieren, um Ihre Untersuchungsberichte individuell anzupassen. Sie können aber auch unsere eigenen Berichte tages-, wochen- oder monatsweise abonnieren. Für weitere Analysen lassen sich die Forensikdaten manuell oder per SIEM-Integration über REST-APIs exportieren.



SCHUTZ VON OFFICE 365-KONTEN MIT FLEXIBLEN RICHTLINIEN

Mit Informationen, die Sie dank unserer detaillierten Forensik erhalten, können Sie flexible Richtlinien erstellen, die auf mehreren Parametern basieren (z. B. Benutzer, Standort, Netzwerk, Gerät, verdächtige Aktivität). Dadurch können Sie zum Beispiel Anmeldewarnungen für Länder auf schwarzen Listen oder für Geräte generieren, die nicht Ihren Unternehmensrichtlinien entsprechen. Wenn Sie einen intensiv genutzten Dienst wie Office 365 überwachen, müssen Sie die Warnungen priorisieren, um eine Überflutung mit Meldungen zu vermeiden. Mit PCAD können Sie Warnungsbenachrichtigungen anhand ihres Schweregrades generieren und dabei jede Benachrichtigung anpassen oder einfach die Standardvorlage nutzen. Und Sie können gefährdete Benutzer genauer überwachen oder sie sperren, wenn eine verdächtige Anmeldung erfolgreich ist.

SCHNELLE BEREITSTELLUNG IN DER CLOUD

Cloud-Plattformen benötigen Cloud-Schutz. Unsere Cloud-Architektur und die Schutzmaßnahmen über Office 365-APIs ermöglichen die schnelle Bereitstellung und sofortigen Mehrwert. Sie können innerhalb von Tagen – nicht Wochen oder Monaten – hunderte oder tausende Benutzer schützen. Als einer der Branchenführer beim Bedrohungsschutz nutzen wir die Cloud, um unsere Software täglich zu aktualisieren, sodass Sie den Angreifern stets einen Schritt voraus bleiben. Unsere Cloud-Bereitstellung bietet auch die notwendige Flexibilität, um Benutzer in jedem Netzwerk oder auf jedem Gerät zu schützen.

WEITERE INFORMATIONEN

Proofpoint Cloud Account Defense unterstützt Sie bei der sicheren Bereitstellung und Nutzung von Office 365. Melden Sie sich unter proofpoint.com/us/products/cloud-account-defense für eine kostenlose Analyse an.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.